IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.: 10/773,069	§		
Filed: February 5, 2004	§	Examiner:	Dada, Beemnet W.
Inventor:	§	Group/Art Unit:	2435
Emrys J. Williams	§	Atty. Dkt. No:	5681-74900
	§		
Title: Method and System for Accepting a Pass Code	§		
	§		

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicants request review of the final rejection in the above-identified application. Claims 1-36, 38-52 and 54 are pending in the application. Reconsideration of the present case is earnestly requested in light of the following remarks. For brevity, only the primary arguments are presented. Additional arguments will be presented if and when the case proceeds to Appeal.

Section 112, First Paragraph, Rejection:

The Examiner rejected claims 1-36, 38-52 and 54 under 35 U.S.C. § 112, first paragraph, as allegedly failing to comply with the written description requirement. The Examiner submits, "The specification does not literally or implicitly exclude 'user input does not include the pass code' … '… without transmitting the pass code to the remote authentication …' … '… without generating the pass code …' … and therefore the claims are rejected under 35 USC 112 First Paragraph." (Final Action, April 09, 2010, p. 2) Applicant respectfully traverses this rejection.

Independent claims 1, 18, 35 and 38

In regard to claims 1-35, 38-52 and 54 the Examiner asserts, "[t]he specification fails to mention or teach the limitation wherein transmitting a response to a remote authorization unit to authenticate a response without transmitting the passcode to the remote authorization unit and without generating the passcode from the user input prior to said transmitting." (Final Action,

April 09, 2010, p. 3). However, as explained below, these features are all clearly supported in the specification.

Figures 1A-1D are described in the Background section of Applicant's specification as examples of systems where the user input does include the actual passcode and/or where the actual passcode is transmitted to a remote authorization service. *See* p. 1, line 11 – p. 3, line 26. The Background section also describes problems with these approaches, such as the risk that the passcode will be intercepted during transmission (*see* p. 3, lines 28-31), and the risk of "sniffer" programs or observation of the passcode when it is being entered (*see* p. 5, line 30 – p. 6, line 19).

The specification then describes how some or all of these problems might be addressed. For example, instead of having the user enter the passcode directly, a challenge-response technique may be used where the user enters a transformation of the challenge instead of the actual passcode. *See* p. 7, line 34 – p. 8, line 17. With this technique, the user input is "received as a set of one or more modifications to be applied to the challenge." Specification, p. 8, lines 28-29. "With this approach, it is less problematic if an adversary observes the user input, since this does not correspond directly to the pass code." Specification, p. 8, lines 6-7. Thus, contrary to the Examiner's assertion, the specification does provide support for "wherein the user input does not include the pass code itself".

In regard to transmitting, the specification does describe embodiments in which the passcode is generated from the user input. However, the specification also describes an alternative embodiment in which the user response to the challenge is transmitted to the remote authorization unit instead of transmitting the passcode itself. Recall that the user response is not the passcode itself, but a set of transformations or modifications. In this case the actual passcode is not generated from the received user response input prior to transmitting. *See, e.g.*, p. 9, lines 18 – 25 ("one option is to calculate the pass code … on the basis of the known challenge and response … Alternatively, the user response may be transmitted to some remote unit … pass code per se might never be calculated." (emphasis added)). Thus, contrary to the Examiner's assertion, the specification does provide support for "transmitting the response to a remote authorisation unit to authenticate the response without transmitting the pass code to the remote authorisation unit and without generating the pass code from the user input prior to said transmitting."

As additional examples of support, Applicant's specification further describes, at Figure 5 and p. 19 lines 29 -31, "The second general approach to validating the user response at step 540 (see Figure 5) is where terminal 300 itself **does not calculate the PIN**, but **rather** provides the user **response** to some other system for verification." Applicant's specification further describes, at p. 22, lines 17-19, "Note that with this approach …, the validation may be performed in some embodiments **without specifically determining the … pass code**."

Accordingly, Applicant's specification clearly describes "transmitting the response to a remote authorisation unit to authenticate the response *without transmitting the pass code to the remote authorisation unit and without generating the pass code from the user input prior to said transmitting*," as recited in Applicant's claims.

Independent claim 36

Claim 36 recites, validating the user on the basis of said response compared to the predicted response, wherein *neither the response nor the predicted response is the pass code.*

In regard to claim 36, the Examiner asserts, "[t]he specification fails to mention or teach the limitation wherein validating the user on the basis of said response compared to the predicted response, wherein neither the response nor the predicted response is the pass code." (Final Action, April 09, 2010, p. 4)

However, Applicant's specification, at p. 9 lines 25-29, which describes, "For example, the security system might predict the response to be entered by a user, based on knowledge of the challenge and the authentic pass code. The **response received from the user can then be tested against this prediction**, and if there is a **match**, the response from the user corresponds to what was expected, and so the user is validated." As described above, the user response is **not** the pass code. Instead, it is a set of transformations or modifications to the challenge. *See, e.g.*, p. 8, line 28 – p. 9, line 7. The predicted response is a means to validate the user response. As described in the Specification, the security system determines whether the predicted response **matches** the user response. Accordingly, the predicted response is expected to be the same as the user response. Since the user response is not the pass code, the predicted response for matching is also **not the pass code.** Accordingly, Applicant's specification clearly describes an embodiment in which *neither the response nor the predicted response is the pass code.*

Independent claims 1, 18, 35, 36 and 38

Claims 1, 18, 35, 36 and 38 recite generating a response from the user input received from the user input device, wherein *the user input does not include the pass code itself.*

In regard to claims 1-36, 38-52 and 54 the Examiner asserts, "[t]he specification fails to mention or teach the limitation wherein the user input does not include the pass code itself." (Final Action, April 09, 2010, p. 4)

Support for this has already been demonstrated above. To reiterate, Applicant notes the following passages of the specification, which describe a user input that is a **response to a machine–generated challenge** and **not** an actual pass code.

p. 7, line 34 – p. 8, line 2: "The method involves providing a user with a machine-generated challenge, and receiving a response from the user. The **response** represents a **transformation from the challenge** provided to the user to a pass code allocated to the user …"

p. 8, lines 6-7: "With this approach, it is less problematic if an adversary observes the user input, since this **does not correspond directly to the pass code**."

p. 8, line 28: "the response from the user is received as a set of one or more **modifications to be applied to the challenge**."

The following specific examples described in Applicant's specification are examples of user inputs that are clearly **not** pass codes:

p. 13, lines 22-24: user input is a sequence of directional buttons: "Up, Up, Up, Up, Right …"

p. 21, line 25: "if the challenge is 1234 and the pass code to be entered is 5352, the received response might be 4127 …"

p. 23, line 31: "It will be appreciated that the challenge-response approach described herein for pass code entry has the significant advantage that **the user does not specifically depress keys corresponding to the pass code itself** on keypad 320. **Instead**, the user only

inputs a **response** that does **not allow the pass code itself to be determined w/o knowledge of the original challenge**."

Accordingly, Applicant's specification clearly describes a user input that **does not include the pass code itself**, as recited in Applicant's claims.

In light of the foregoing remarks, Applicants submit the application is in condition for allowance, and notice to that effect is respectfully requested. If any extension of time (under 37 C.F.R. § 1.136) is necessary to prevent the above referenced application from becoming abandoned, Applicants hereby petition for such an extension. If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert & Goetzel PC Deposit Account No. 501505/5681-74900/RCK.

Respectfully submitted,

/Robert C. Kowert/
Robert C. Kowert, Reg. #39,255
Attorney for Applicant

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8850

Date: July 9, 2010